ieri
Information Economy
Research Institute

ITコーディネータ実務研究会

2010.1.23.

クラウド時代の情報セキュリティ最前線

クラウドコンピューティングの光と影

－中小企業の経営にいかに生かすか－

ieri
Information Economy
Research Institute

株式会社 情報経済研究所
情報セキュリティコンサルティング

代表取締役 勝見 勉

〒227-0043
横浜市青葉区藤が丘2－1－3－826
Tel/Fax: 045-972-6548
携帯: 090-8753-4306
e-mail: info-economy@xvg.biglobe.ne.jp

Info-economy@xvg.biglobe.ne.jp

公認情報システム監査人(CISA)
ISMS審査員補
情報セキュリティ監査アソシエイト
情報セキュリティアドミニストレータ

今日お話しすること

- クラウドコンピューティングとは
- クラウドのセキュリティ
  - クラウドセキュリティの諸説
  - 全体を整理すると:
  - クラウド環境の攻撃モデル
  - クラウドのインシデント事例
- クラウドとどう付き合うか

クラウドコンピューティングの定義

クラウドとは：（現時点の共通理解）

- インターネット上で提供されるコンピューティングサービス
- ユーザに対しては、アプリケーションまたはコンピュータとして“見える“
- 従量課金モデルで必要なだけ利用可能
- システムの内容やハードウェアの構成･存在はユーザからは見えない（雲の中）
- 提供される切り口として、SaaS、PaaS、IaaSなどがある
- コンピューティング技術としては、分散処理、仮想化等が用いられ、ネットワーク上に分散した資源を、仮想的に一つのマシンのように見せ、使わせる

Cloud 3つの “aaS”

SaaS: Software as a Service

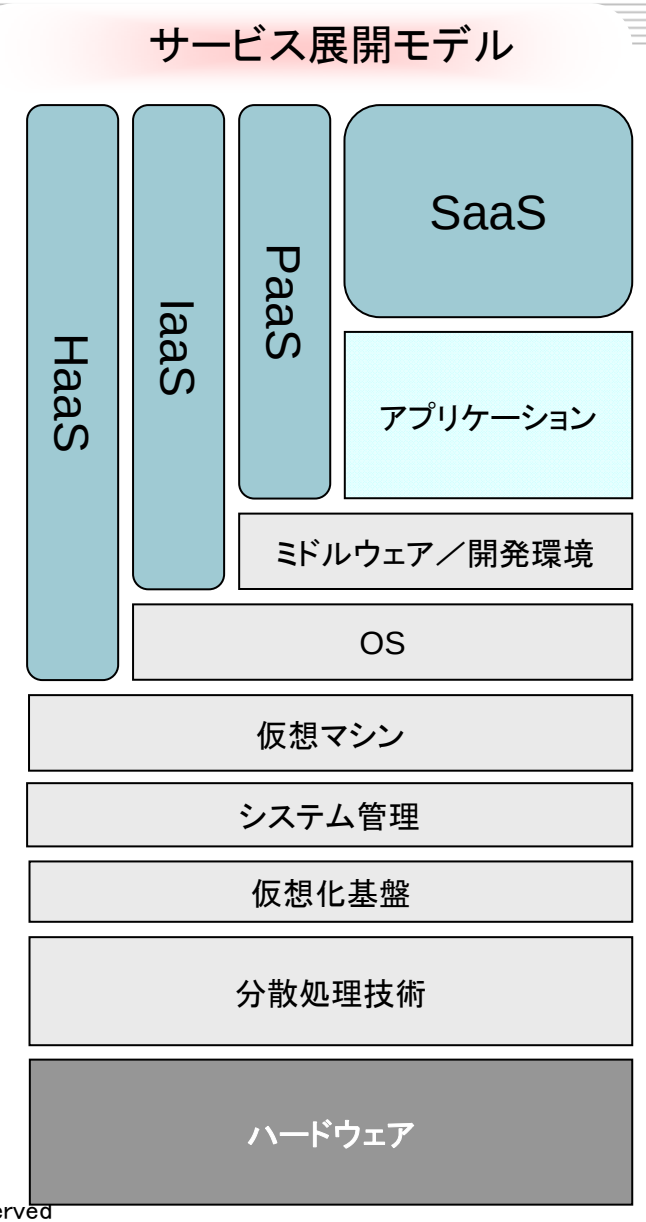
・アプリケーションの機能をサービスとして提供 （プラットフォームはCloudでなくてもよい）
・クラウド上のSaaSがクラウドコンピューティングとして注目（UC Berkeley Model）
・ユーザは出来合いのアプリを、一部カスタマイズしながら利用する
・典型例は Salesforce.com, Google Apps ・ラクラスのHRサービスもこの例

PaaS: Platform as a Service

・アプリケーション構築環境（言語、ツール、ユーティリティ等）を提供
・ユーザはアプリケーションを自作の上、利用する
・典型例は Force.com, Google App Engine, MS Azure

IaaS: Infrastructure as a Service

・生のコンピューティング資源を提供
・ユーザは自分でシステム開発の上、利用する（開発ツール等は制約がない?）
・典型例は Amazon EC2, S3 MS-SSDS



クラウドの特徴

構造上の特徴

分散処理

- ネットワーク上に散在するコンピュータを複数接続して並列処理する
- グリッドコンピューティング／並列処理

分散ストレージ

- ネットワーク上に散在するストレージを複数接続して一台のディスクのように利用する

ネットワーク＝システムバス

- システムバスはネットワーク

仮想化環境

- このような分散した資源を統合して仮想的に1台のコンピュータとして扱う
- その上に仮想的なマシンを複数立上げ、各マシンを独立したコンピュータとみなして利用する
- 各仮想マシンは論理的に分離されている

メリットとデメリット

拡張性と柔軟性

- 処理量に応じ、使用する資源の量を柔軟に増減できる（H/Wの追加投資不要）

初期投資不要

一時的増強も可能

開発期間短縮

変更改良が容易

使っただけ払う

分散環境で障害に強い

確率・頻度不明

専門家によりセキュリティに強い

危険への露出度も大きい

データの物理的所在が不明

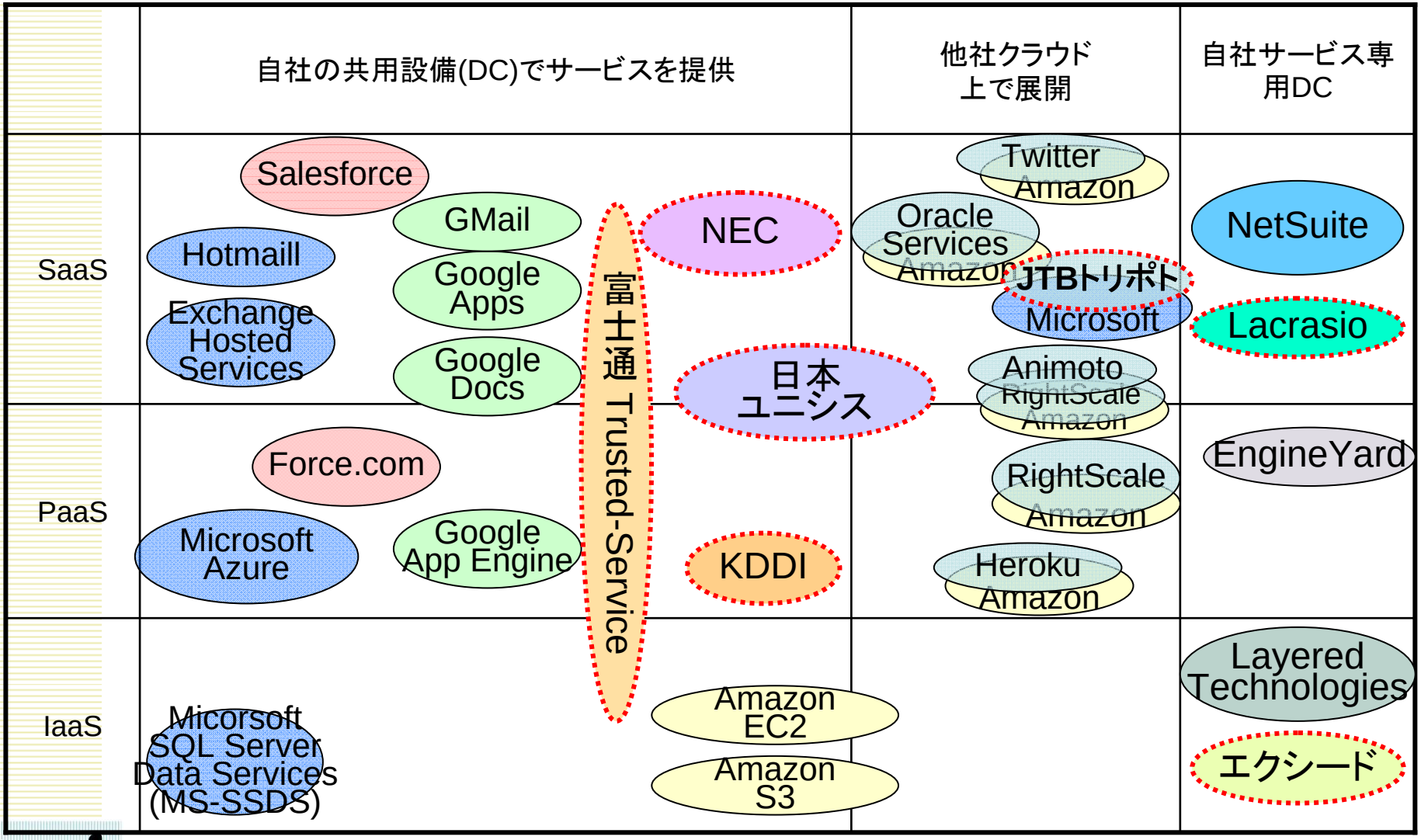
データやプロセスの相互隔離の保障

セキュリティや信頼性の評価指標が未確立

単一事業者への依存過多＝ロックイン問題

自社や第三者とのシステム・データ連携問題

パブリッククラウドの サービスモデルの分布



: 日本の事業者

SaaSとCloud：どう使う、どこで使う

ユーザ / システムサービス	中小企業	大企業		重要インフラ		
	システム全般	業務系	基幹系	業務系	基幹系	コア系
データセンター / プライベートクラウド / パブリッククラウド — SaaS	◎ 自前より安全 自前より安い 開発負担小 開発期間短 運用容易 スケーラブル	メリットは左に同じ ◎ 対象データを限定 SLA	可用性、使い勝手 × データのCIA、所在地リスク	△	×	×
パブリッククラウド — PaaS Iaas	○ 特定用途 開発負担小 開発期間短 運用容易	◎ 同上	△特定用途条件限定	○	×	×
地域・業界等特定領域クラウド*	◎ SaaSのメリット 安心・柔軟	◎ 同左	◎ 自グループ自業界等	○	△	×
プライベートクラウド	× コストメリット無し	◎ 垂直立上拡張性	◎ 垂直立上拡張性	◎	◎	△
独自・固有システム	―	―	―	―	○	◎

*J-SaaSのように国、県等地域共用や、業界共用のクラウド基盤

セキュリティ課題の整理

	制度面・ビジネス（取引）面 及び　クラウドの利活用	技術的側面 システム	技術的側面 データセンタの管理・運用
情報セキュリティ	データセンター施設のセキュリティ ー立地、自然災害、ユーティリティ確保 ー物理的アクセス制御、モニタリング	アーキテクチャ自体に関わるセキュリティ ー仮想化環境 ーハイパーバイザー ー大規模分散システム（グリッド） ープロセス間の隔離	運用の管理 ーオペレータのアクセス管理 ーシステム特権管理 ー不正アクセス対策 ーインシデント対応 ーパッチ・脆弱性・ウイルス対策ソフト管理 ーアプリケーション管理
	クラウドーユーザ間通信のセキュリティ ー通信路の信頼性、通信品質確保 ー通信の秘匿性・セキュリティ	データストレージのセキュリティ ーストレージの物理的場所（災害対応、バックアップ、地政学的リスク） ーデータ相互間の隔離	
	情報のライフサイクル管理		情報のライフサイクル管理
	暗号と暗号鍵管理		
	利用端末のセキュリティ	暗号化ソリューション：通信、データ、操作	
	ユーザ認証とアクセス管理の仕組み、モニタリング		
事業継続管理	クラウド事業者の存続性	ハードウェアの信頼性・冗長性	
	クラウド事業者の経営とガバナンス	災害復旧計画と災害対応	
	クラウド事業者のBCP	システム及びサービスの可用性・信頼性	
コンプライアンス	法制度的要請への対応 ー内部統制 ー個人情報保護法 ーFISMA　等	監査可能性と対応（ユーザ、第三者、行政・司法当局） デジタル・フォレンジック対応	
	データの保管場所と立地国の法制度・プライバシー法制の影響		
オペレーション	SLA標準／ガイドライン		サービスレベルの保証 ー処理能力・拡張性 ーストレージ要領・拡張性
	データ及びアプリケーションのポータビリティ／ロックイン		
	相互運用性と標準化（クラウドークラウド間、クラウドーユーザ環境間）		
			データ転送のボトルネック

パブリッククラウド利用時の留意事項

1 データは預けない

－洩れては困るデータ
－なくなっては困るデータ

ローカルバックアップ

2 一定時間以上止まって困る用途には使わない

－申込受付システム
－受発注システム

「SLA稼働率保証99.5%」が意味するもの：
・年間44時間の停止までは、値引きしませんよ!
・稼働時間の率99.5%保証ではない!!!

3 SLA神話には乗らない

－Noと言ったら使えない
－事故が起きない保障は誰にもできない

S/Wライセンス：Noと言ったら使えない
ファイルDL：Noと言ったらできない

4 SSL通信は絶対

－平文通信は避ける

5 事故の多い事業者は避ける

－対応が遅い
－復旧が遅い

自営のシステムでも事故は起こる
運用レベルは専門事業者のほうが高い

自社でやるよりは高いセキュリティ対策レベル

参考資料のURL

- クラウドのセキュリティ課題に関するレポート等
  - http://csrc.nist.gov/organizations/fissea/2009-conference/presentations/fissea09-pmell-day3_cloud-computing.pdf
  - http://www.cloudsecurityalliance.org/
  - http://www.eecs.berkeley.edu/Pubs/TechRpts/2009/EECS-2009-28.pdf
  - http://www.gartner.com/DisplayDocument?id=685308 （有償）
  - http://www.meti.go.jp/information/downloadfiles/c90710b01j.pdf
  - http://www.ipa.go.jp/about/news/event/ipax2009/pdf/IPAX2009_security_matsumoto.pdf
- 政府におけるクラウド関係の研究会等
  - http://www.meti.go.jp/committee/kenkyukai/k_8.html
  - http://www.soumu.go.jp/main_sosiki/kenkyu/smart_kuraudo/17306.html

講師自己紹介

株式会社 情報経済研究所

代表取締役 勝見 勉

e-mail: info-economy@xvg.biglobe.ne.jp

情報セキュリティコンサルタント

IPA嘱託・研究員(2004～)

IPAセキュリティセミナー講師

JNSA理事・幹事

セキュリティ市場調査WGリーダ

日本セキュリティ監査協会幹事

普及促進部会CAIS促進WGリーダ

ISEPA(教育事業者連絡会)広報部会主査

公認情報システム監査人(CISA)

ISMS審査員補

情報セキュリティ監査アソシエイト

情報セキュリティアドミニストレータ

日本セキュリティマネジメント学会会員

デジタルフォレンジック研究会会員

【情報セキュリティに関する職務経歴】

◆日新電機(1995～2001)

ファイアウォール等セキュリティ対策機器等の輸入販売

BS7799規格の紹介・利用促進

◆シマテック(2001～2004)

総合セキュリティ対策の促進

◆グローバルセキュリティエキスパート(2005～2006)

侵入検査、技術コンサルティング事業の開発推進

◆リコーヒューマンクリエイツ(2006～2008)

ISMS、PM認証取得支援 、情報セキュリティ教育事業の推進

リコーグループのISMS推進

CISA受験対策教育コースの開発

ISMSユーザーズグループメンバーとして実践研究

【情報セキュリティに関する調査実績及び専門性】

- JNSA「情報セキュリティ市場調査」(経済産業省委託事業)主査(2004～2009各年度)
- JNSA中小企業セキュリティ対策指導者育成セミナー(経済産業省委託事業)講師
- IPA情報セキュリティ産業構造調査主査
- IPA「情報セキュリティ白書」執筆委員
- IPA情報セキュリティセミナーマネジメント編テキスト改訂執筆
- ISEPA「情報セキュリティ人財アーキテクチャガイドブック」執筆編集
- IPAクラウドセキュリティ勉強会主催
- IPAクラウドコンピューティング社会基盤研究会参画